BUFFALO

AirStation G54

54Mbps Wireless Bridge Base Station

User Manual

WLA2-G54C

INTRODUCTION

1.1 AirStation 54Mbps Bridge Base Station (WLA2-G54C)

This User Manual introduces you to the High-Speed AirStation 54Mbps Bridge Base Station and will assist you with the more advanced features of the product.

The AirStation 54Mbps Bridge Base Station ,WLA2-G54C, is a wireless network access point that can be added to an existing network (LAN) to create a wireless network or added to an existing WLAN to extend the range of the WLAN. The WLA2-G54C complies with the IEEE 802.11g wireless standard and is interoperable with the IEEE 802.11b wireless standard. IEEE 802.11g technology features longer range than IEEE 802.11a and greater bandwidth with data rates up to 54 Mbps in the turbo mode. The WLA2-G54C supports Wi-Fi Protected Access™, AES, 802.1x and WEP for security. The WLA2-G54C supports the Wireless Distribution System (WDS) and can be used as a multi-functional bridge/link between wired and wireless LANs. The WLA2-G54C has a built-in 10/100M 4-port switch to incorporate features of wired and wireless networking environments.

1.2 AirStation Wireless Network Features

Summary of the AirStation WLA2-G54C features:

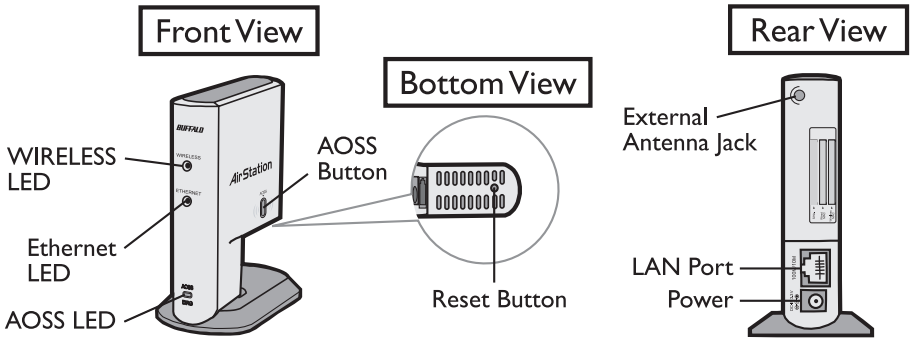
- AOSS automatically creates a secure connection between your AOSS Access Point and client.
- Wi-Fi™ (Wireless Fidelity) certified AirStation will communicate with other Wi-Fi compliant 802.11g wireless LAN products.
- Wi-Fi Protected Access™ (WPA), AES, 802.1x and WEP for protecting data.
- Automatic Transmit Rate Select mechanism transmits at speeds of 24, 12, 11, 5.5, 2 and 1 Mbps.
- Supports turbo mode of 36, 48 and up to 54 Mbps.
- Wireless Bridge System (WDS) support for multi-point communication.
- Ability to set a fixed data rate for faster than 11Mbps ignoring 802.11b legacy devices.
- Auto roaming, supports seamless roaming over multiple channels.
- Wi-Fi Protected Access™ support.
- EAP-TLS, expanding the 802.1x authentication method.
- Up to 128bit Wired Equivalent Privacy (WEP) data encryption.
- Packet Filtering for eliminating unwanted communications.
- Syslog transmits some or all system activities to a central Syslog server.
- Extended range, with optional add-on 2.4GHz antennas.
- Auto Media Dependent Interface/Crossover (MDI/X) port, allows connection by standard and crossover CAT5 cables.
- Optional external 2.4 GHz antennas for boosting range and signal quality.
- Improved resistance to environmental conditions.

1.3 AirStation 54Mbps Bridge Base Station Package

The AirStation WLA2-G54C package consists of the following items.

1. WLA2-G54C
2. AC adapter with Int'l Adapters
3. CAT5 straight cable
4. Quick Setup Guides
5. WLA2-G54C Utility CD with Manuals
6. Warranty Statement
7. Wall mounting kit

1.4 Product Views



1.5 About the AirStation CD

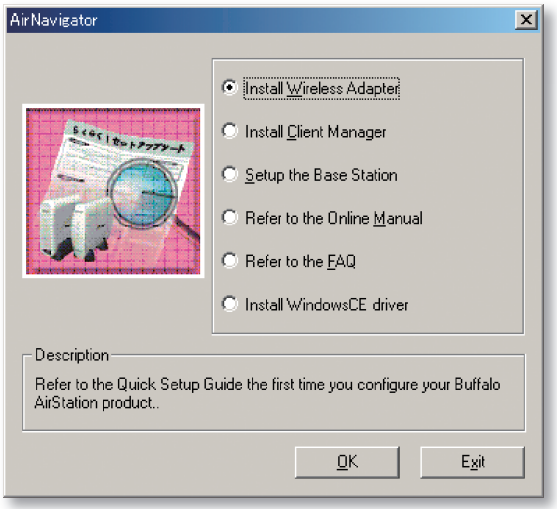
Prior to copying or installing the software, please read the Software License Agreement "license.txt", located in the root folder of the CD. By installing, copying or using the AirStation software, you are consenting to the terms of this agreement. If you do not agree to all of the terms of the Software License Agreement, do not download, copy or install the AirStation software.

It is the policy of Buffalo Technology to improve products as new technology, components, software and firmware become available.

Before you proceed with the installation of this product, please consult the Buffalo website (**indicated last page**) to download and install the latest software for your product.

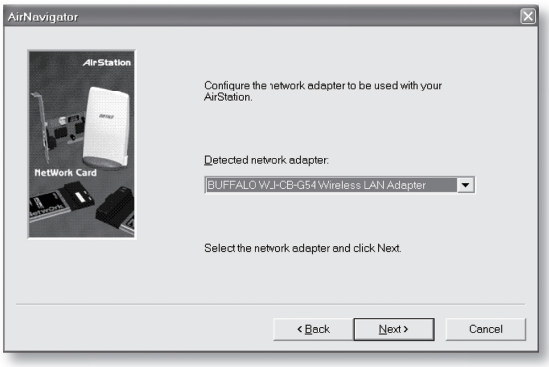
BASIC SETUP

2.1 Using AirNavigator For easy setup, the WLA2-G54C CD contains a web-based utility, AirNavigator. Use it to set up the wireless LAN environment for both AP and PC (client). The system requires Explorer 4.0 or higher, or Netscape Communicator 4.0 or higher.

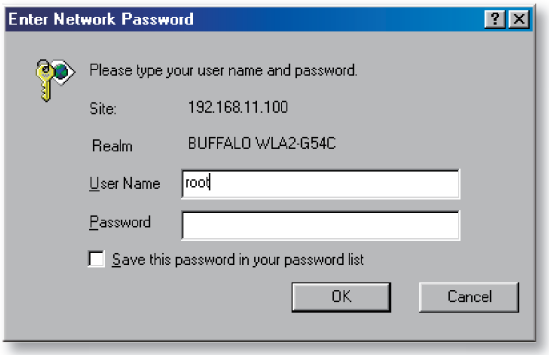


To set up the parameters manually, refer to Chapter 3. Before installation, verify the PC is set up for browsing the Internet.

1. Insert the AirNavigator CD into the CD drive. The following screen will appear. For AirStation setup, select "Setup the BaseStation" and click **OK**.

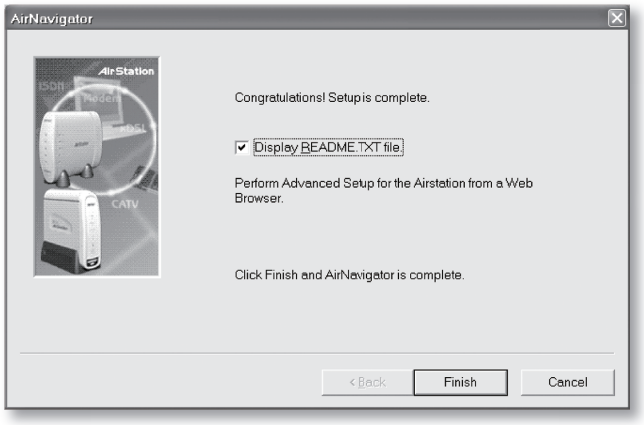


2. The Network Adapter confirmation screen will appear. Verify the adapter shown matches that of the PC.



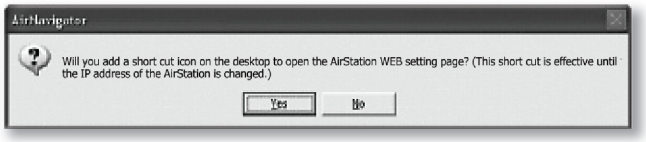
3. A login screen will appear.
- Enter "root" as the User name.
- Leave the Password box blank (do not enter anything into the Password box) and click OK.

If the following screen is shown, connection to the WLA2-G54C is complete.



If the following screen is shown, connection to the WLA2-G54C is complete.

4 Click **Finish**.


AirNavigator
Will you add a short cut icon on the desktop to open the AirStation WEB setting page? (This short cut is effective until the IP address of the AirStation is changed.)
Yes
No

5 To place a shortcut icon on the desktop, click **Yes**. Otherwise, click **No**.

STANDARD SETTINGS

3.1 Introduction

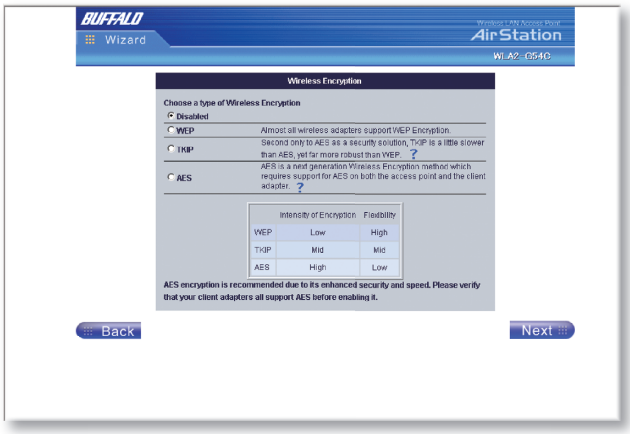
Setting up the AirStation parameters using a Web Browser requires basic wireless configuration knowledge. For Advanced settings and explanations of each parameter and its use, see **Chapter 4.**

3.2 Setup Overview

The WLA2-G54C is configured to function right out of the box. Simple settings for security and MAC Address registration are offered in this section, Specialized setups for security, filtering and other features will be explained in later sections by clicking the **Advanced** Button.

3.3 Open the Setup Screen

• Click "Encrypt the wireless communications (WEP/TKIP/AES)" to enter Encryption setting to protect your wireless data.


BUFFALO
Wizard
AirStation
WLA2-G54C
Wireless Encryption
Choose a type of Wireless Encryption
Disabled
WEP
Almost all wireless adapters support WEP Encryption.
TKIP
Second only to AES as a security solution, TKIP is a little slower than AES, yet far more robust than WEP.
AES
AES is a next generation Wireless Encryption method which requires support for AES on both the access point and the client adapter.
Intensity of Encryption
Flexibility
WEP Low High
TKIP Mid Mid
AES High Low
AES encryption is recommended due to its enhanced security and speed. Please verify that your client adapters all support AES before enabling it.
Back
Next

Select the Type of encryption and click "Next" to input a password or encryption code to protect wireless communications.

WEP - It is possible to enter up to 4 different WEPs. The WEP key must match between two parties for secure communications.

Examples of WEP key:

64bit ASCII: 5 digits of alphanumeric characters, "ab34Y"

128bit ASCII: 13 digits of alphanumeric characters, "123456abcdef7"

64bit HEX: 10 digits, using characters 0-9 and a-f, "00234ABCDE"

128bit HEX: 26 digits, using characters 0-9 and a-f, "20123456789abcdeabcdeab cde"

TKIP (Temporal Key Integrity Protocol) - A WEP expanded encryption technique. TKIP has greatly improved WEP's weaknesses by rotating secret keys between every packet.

Characteristics:

• The Initialization Vector is expanded from 24 bits to 48 bits.

• The Initialization Vector is randomized.

• Uses a different RC4 key for every packet

AES (Advanced Encryption Standard) - A next generation encryption technique discussed by the IEEE 802.11i committee.

TKIP improves WEP's weakness, however AES also changes the encryption method away from the weaker RC4 style.

Throughput decreases 10 to 20 percent when TKIP software encoding is used. AES doesn't decrease performance at all because it uses a hardware co-processor.

Characteristics:

• USA government uses same encryption method. AES encryption has not been hacked to date.

• The hardware co-processor contributes less throughput loss then other forms of encryption.

3.4 Simple Setting for Wireless MAC Filter

• Click "Wireless MAC Filter" and then "Next" to set up MAC address restriction in LAN.

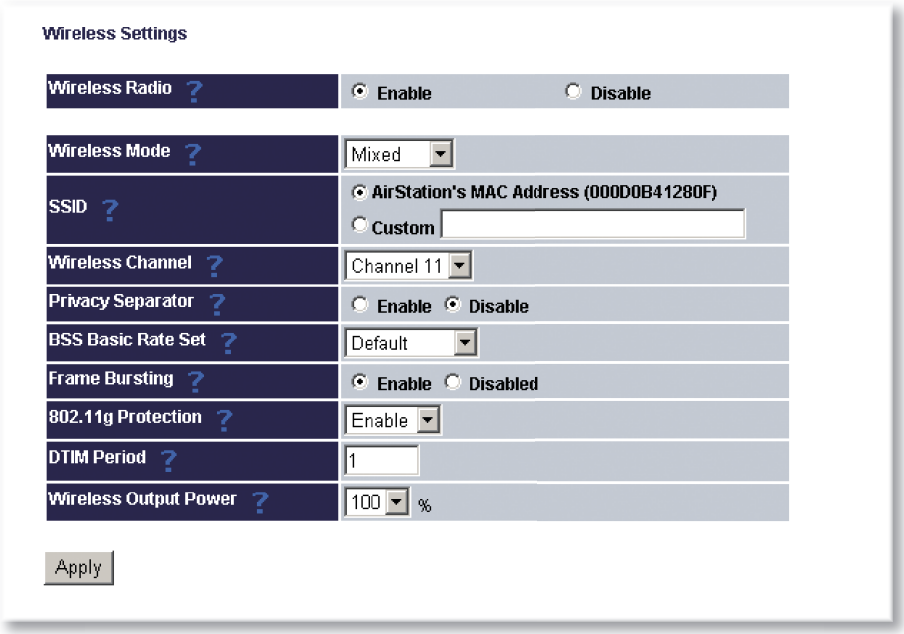
Input MAC addresses that is to be allowed to communicate.

USING AIRSTATION FOR ADVANCED CONFIGURATIONS

Although your AirStation will function fine using only the settings from Section 3, you may wish to explore more advanced options. This chapter explains each parameter in the **Advanced** button. Click the **Top tab** and click the **Advanced** button.

4.1 LAN Setting

4.1.1 Wireless



Wireless Radio - Enable or disable wireless communication

Wireless Mode - Select one of the following:

Mixed - Allows communication of 11g and 11b devices. Communication speed will drop to 11Mbps when 11b devices are connected.

11g-only - Boosts 11g devices to turbo 54Mbps mode.

11b-only - Use only the IEEE802.11b (11Mbps WiFi compatible) standard.

SSID - Allows administrator to alter the SSID of the AirStation. Default SSID is the LAN MAC Address. To communicate with a specific AP only, the AP's SSID must be entered in the client PC. The client PC looks for the specific AP (or SSID) for wireless communication. Use up to 32 alphanumeric characters for the SSID (case sensitive).

■ Note: **Roaming** - When multiple AirStations have an identical SSID, and WEP client PCs may Roam between the AirStations.

Wireless Channel - Select the channel used for wireless communication. There are 11 overlapping channels. Channels 1, 6 and 11 are non-overlapping.

If there are multiple APs in close proximity using the same channel, there may be interference. In this case, change to a non-overlapping channel.

■ Note: This parameter is automatically set in the client computer.

Privacy Seperator - Select Use or do not use to block communication between each wireless LAN PC on the wireless network. If you choose to use, every wireless LAN PCs that is associated to the same AirStation can not communicate with each other. Even if this function is used, wired LAN PCs can communicate with wireless LAN PCs.

BSS Basic Rate Set - Determines the rate at which data will be transmitted between devices on the network. The default BSS on the AirStation will allow high transmission rates for 802.11g products while still accommodating the lower transmission rates of 802.11b and 802.11 wireless clients.

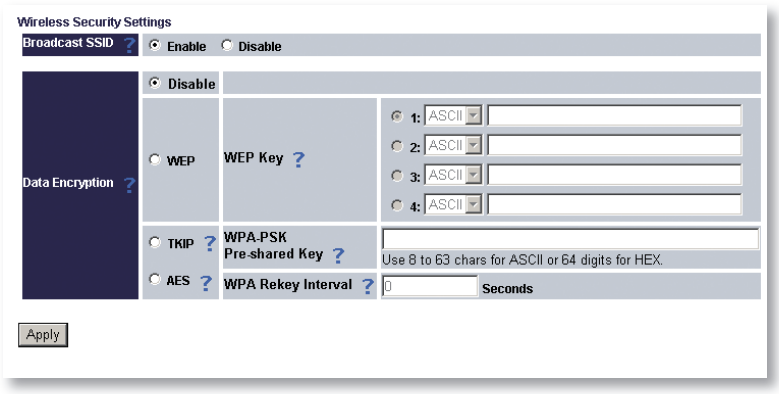
Frame Bursting - Increase IEEE802.11g communication throughput by transferring packets continuously. However, the following condition effects this function. The client wireless LAN adapter must support Frame Bursting feature too. When multiple wireless clients use Frame Bursting feature, the throughput might not increase

802.11g Protection - When this function is enabled, the AirStation requests IEEE802.11b devices to stop communication for a while prior to starting IEEE802.11g communication. If communication speed is decreased, this setting improves total throughput with existing IEEE802.11g and IEEE802.11b standard devices,. The throughput decreases if only IEEE802.11g standard devices exists.

DTIM Period - A transmits beacon signals to nearby clients at a preset interval. This parameter sets the beacon transmission interval time (1-255 sec.). Selection of a larger number may conserve energy for the client PC (when client power management is enabled), but may delay wireless communication. The default value of 1 is recommended.

Wireless Output Power - Adjust the power ouput power of the radio.

4.1.2 Wireless LAN Security



Broadcast SSID - This setting turns off SSID broadcasting which makes the AirStation invisible to client surveys. Clients will have to be manually configured to connect to an AirStation with SSID broadcasting turned off.

The only options are to allow or deny connections for these types of clients, thus, wireless networks requiring security should mandate an encryption policy to preserve security if SSID broadcasting is allowed.

Data Encryption - Select encryption type of wireless data communication.

Disable - Disable data encryption.

WEP - Using WEP encryption. Encryption key should be entered. When an encryption standard is implemented into a wireless network, a WEP key is used between the client and access point to successfully encrypt, transmit and decrypt data. For this reason, the same WEP key must be used for communication by the client and the access point with which it is attempting to establish a connection session. An access point and client may both carry multiple WEP keys. It is necessary for not only the WEP keys to match, but also the WEP key's location or number. If a wireless client can not support multiple WEP keys, the AirStation's must be configured to transmit key number 1 for a connection to take place.

■ WEP Key Input Formats

64bit ASCII: 5 digits of alphanumeric characters, "ab34Y"

128bit ASCII: 13 digits of alphanumeric characters, "123456abcdef7"

64bit HEX: 10 digits, using characters 0-9 and a-f, "00234ABCDE"

128bit HEX: 26 digits, using characters 0-9 and a-f, "20123456789abcdeabcdeabcde"

TKIP - Using TKIP(Temporal Key Integrity Protocol) for data encryption.

AES - Using AES(Advanced Encryption Standard) for data encryption.

WPA-PSK - Authenticate with the AirStation using WPA-PSK (Pre-shared key), and then encrypt data using TKIP or AES. The wireless client's settings must use the same encryption method and key. Select "TKIP" or "AES" as the [Data Encryption].

■ WPA-PSK Input Formats

8 to 63 characters in ASCII or 64 digits hexadecimal key.

Example 1: [airstation-WPA-PSK]

Example 2: [0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef]

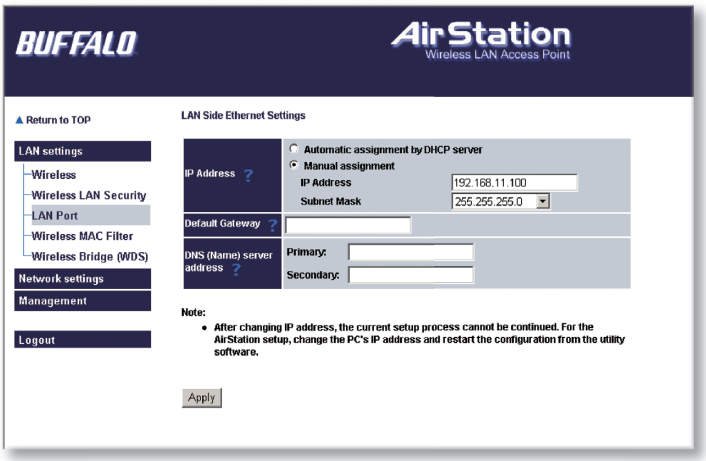
WPA Re-key interval - When TKIP or AES is selected, the encryption key is renewed at this interval. This interval is in seconds; the range of acceptable values is 0-3600.

If 0 is entered, key is never renewed.

■ **Note:** The lower the rekey interval is, the more often a rekey happens. Setting this number low may slightly affect your performance.

4.1.3 LAN Port

Set LAN interface parameters.



IP address - Allows administrator to select whether AirStation is assigned an IP address by a DHCP server or specify a static IP and Subnet Mask for the LAN side of the AirStation.

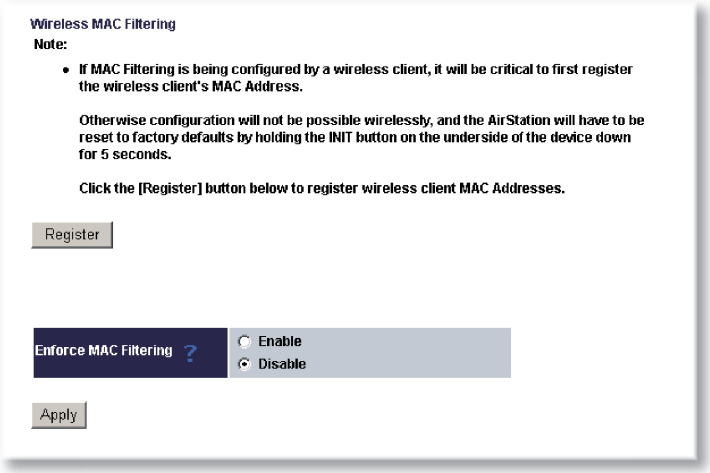
■ Note: If the AP's IP address is changed to a different range, the setting PC's IP must be changed to the same range to continue configuration. Then restart the setup session from the AirStation utility screen.

Default Gateway - Allows administrator to use the Default Gateway address (the AirStation's IP address), assign a specific Gateway address, or block clients from Gateway notification.

DNS (Name) server address - Allows administrator to use the default DNS address (the AirStation's IP address), assign specific DNS addresses, or block clients from DNS address notification.

4.1.4 Wireless LAN Computer Limitation

This option limits the PCs allowed a wireless connection to the AirStation. It is used to control the wireless connections to the AirStation.


Wireless MAC Filtering
Note:
If MAC Filtering is being configured by a wireless client, it will be critical to first register the wireless client's MAC Address.
Otherwise configuration will not be possible wirelessly, and the AirStation will have to be reset to factory defaults by holding the INIT button on the underside of the device down for 5 seconds.
Click the [Register] button below to register wireless client MAC Addresses.
Register
Enforce MAC Filtering
Enable
Disable
Apply

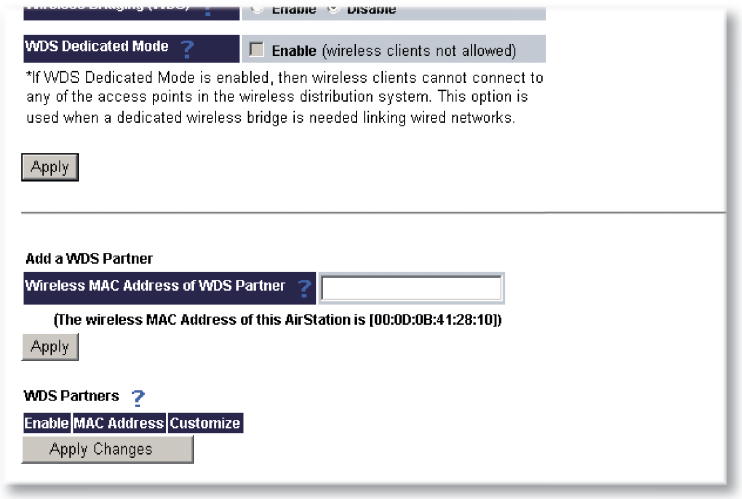
Enforce MAC Filtering - Select Enable to restrict the connection and Disable for open access. Register your client PC's MAC address before selecting Set.

MAC address to be registered - MAC access restriction set up in LAN. Input the MAC addresses that to be allowed to communicate.

MAC address list - Display a table list of all MAC addresses.

4.1.5 Wireless Bridge (WDS)

Wireless Distribution System allows the wireless connection of access points to extend a wiredor wireless infrastructure to locations where cabling is not possible or too expensive to implement.


WDS Dedicated Mode
Enable (wireless clients not allowed)
*If WDS Dedicated Mode is enabled, then wireless clients cannot connect to any of the access points in the wireless distribution system. This option is used when a dedicated wireless bridge is needed linking wired networks.
Apply
Add a WDS Partner
Wireless MAC Address of WDS Partner
(The wireless MAC Address of this AirStation is [00:0D:0B:41:28:10])
Apply
WDS Partners
Enable
MAC Address
Customize
Apply Changes

Wireless Bridging (WDS) : Select **Enable** to allow WDS mode between AirStations or **Disable** to block communication between AirStations.

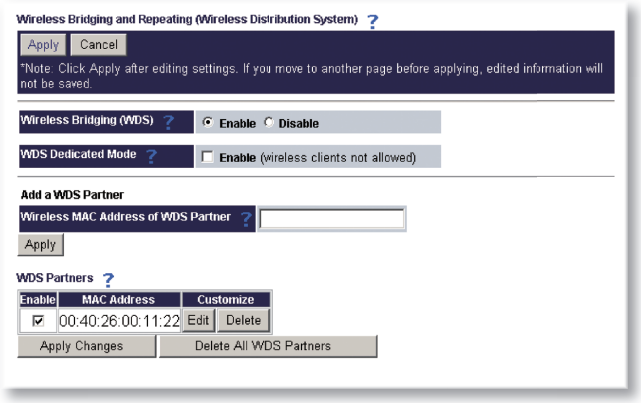
WDS Dedicated Mode : Select Enable to disable wireless PCs from communicating with the AirStation.

■ Note: Both AirStations must support WDS to communicate with each other. WDS process must be repeated with other bridge access points.
Example: AP1 MAC Address is entered into AP2; AP2 MAC Address is entered into AP1;

Add a WDS Partner : Allows administrator to register the wireless MAC address of AirStations for (WDS) point-to-point or point-to multipoint communication between AirStations. The MAC address to enter is found in the Management section, under System Information/Wireless MAC address section. The WDS function must be set to **Enable**. The MAC address is 12 characters long.

Enter the Wireless MAC address in the form of two characters separated by a colon and click **Apply**. Up to six sets may be registered.

WDS Partners : Once settings have been added to the WDS configuration screen, the MAC Address of associated Access Point(s) will be displayed.



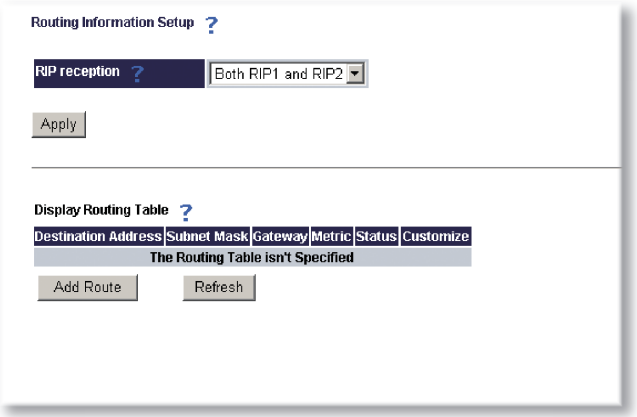
Click Apply to confirm settings.

4.2 Network Setting

4.2.1 Routing Setup

Routing is the path data packets take between devices on the network.
A route is governed by the routing table, a copy of which exists on each network device.
If the device you are trying to communicate with does not exist on the network, the data packet is sent to the default gateway to look outside the network for the device.

The Routing Information Protocol (RIP, also called RIP1) is used to exchange data between routers.
Similarly, if you allow the AirStation to receive RIP information, the AirStation's routing table will incorporate the information it receives from the other routers. RIP2 is an updated, extended version of RIP

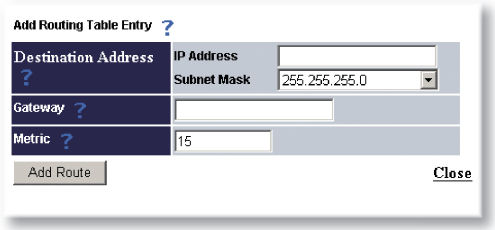


RIP reception - This determines the type of RIP information to receive.

Select None, RIP1, RIP2 or both. Default setting is Both RIP1and RIP2.

Display Routing Table (Entries) - Allows administrator to delete routing information.
This displays the current manual additions to the routing table.

Click [Add Route] to enter new routing rule.



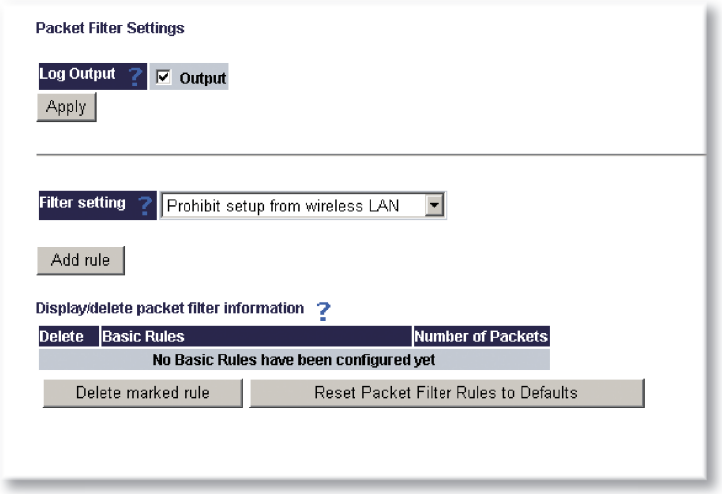
Add Routing Table Entry

- **Destination Address** - Network IP address and subnet mask.
- **Gateway** - Address through which the packet passes before it reaches the destination address.
- **Metric** - Number of bridges (1-15) to be passed before the packet reaches its destination.

4.2.2 Packet Filter - This feature limits configuation on the AirStation Bridge Base Station

Log Output - Activates the packet filter log.

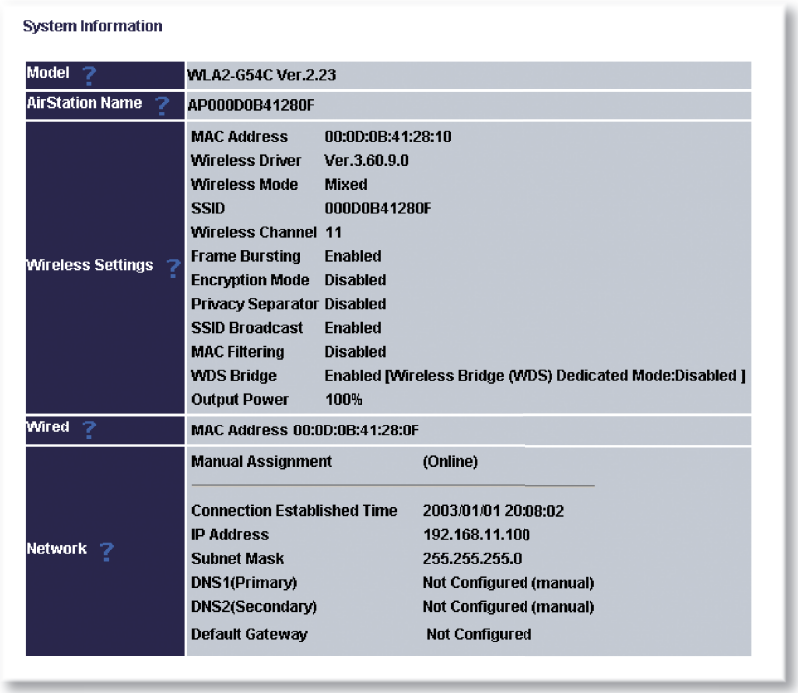
Filter setting - Choose type from pull-down menu.



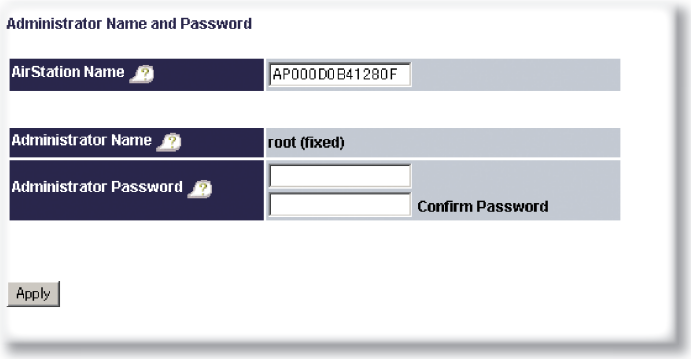
Display/delete packet filter information - The current active filter rules are displayed, and rules shown here may be deleted.

The 'Delete marked rule' button will delete any rules marked, while the 'Reset Packet Filter Rules to Defaults' resets all rules to the factory default settings.

4.3 Management (Network Diagnosis Settings)



4.3.1 System information - Displays System Settings and information including wireless MAC Address needed for WDS mode.



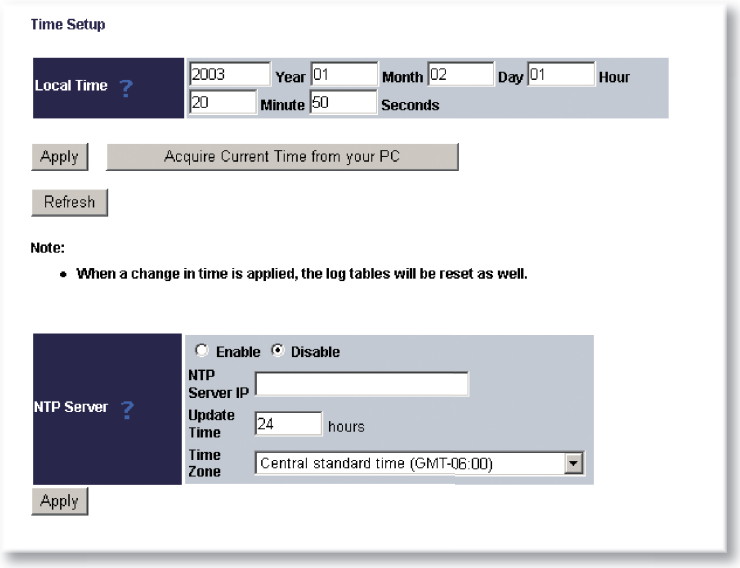
4.3.2 Name and Password

AirStation Name - When using Client Manager and multiple AirStations, select a unique name to make it easier to identify each AirStation.

Administrator Name - "root", cannot be changed

Administrator Password - Allows the administrator to enter an administrator password to restrict access to the setting screens. Enter new password. Enter up to eight alpha-numeric characters (case sensitive) and confirm password

If password is forgotten or misplaced, The WLA2-G54C can be returned to all the factory default settings by holding down the INIT button on the back of the unit for three seconds.



4.3.3 Time setup

Local Time - Enter the current date and time, and click **Apply.**

NTP Server- Select **Enable** or **Disable.**

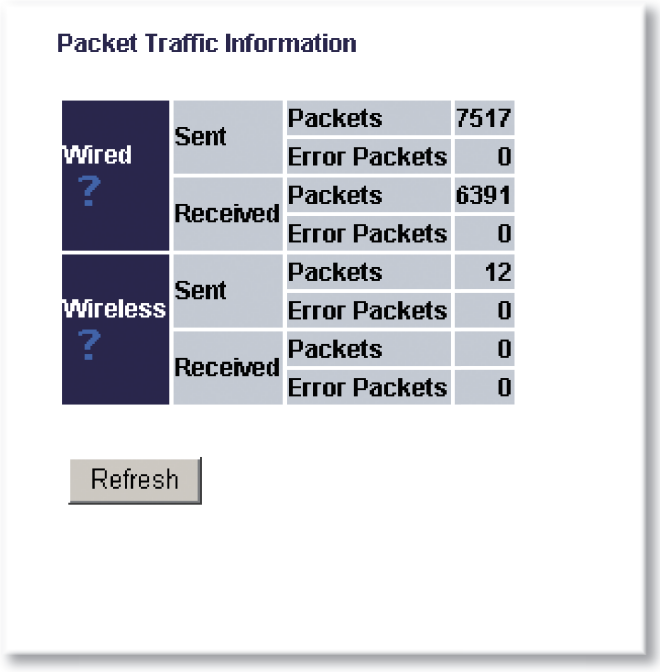
■ Note: If NTP is used, time is set automatically.

NTP server IP - Enter the NTP server IP

Update Time - Enter the time interval for time check frequency

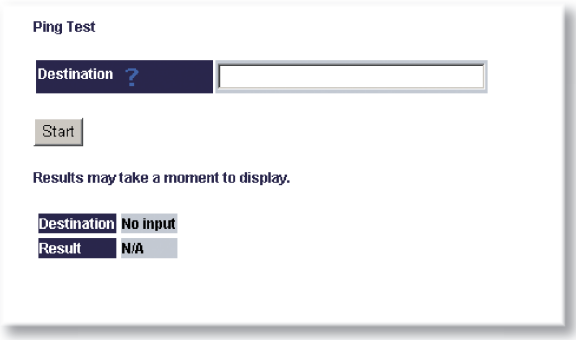
Time Zone - Select local time zone

Click **Set.**



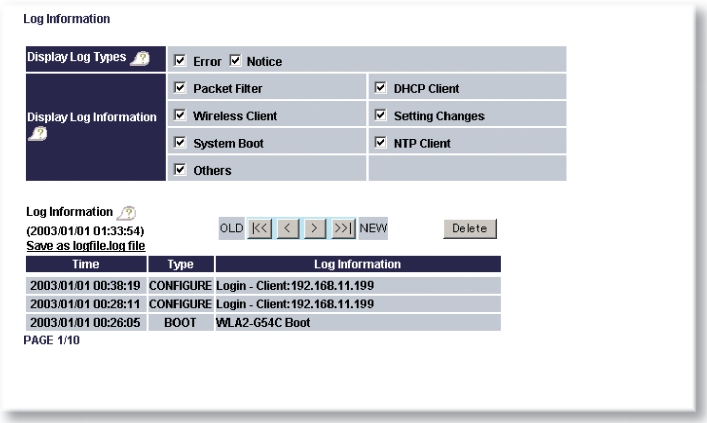
4.3.4 Packet Traffic Information

Displays number of packets sent and received for wired and wireless LAN traffic.



4.3.5 PING Test

Destination - Enter IP address for test and click **Start.**

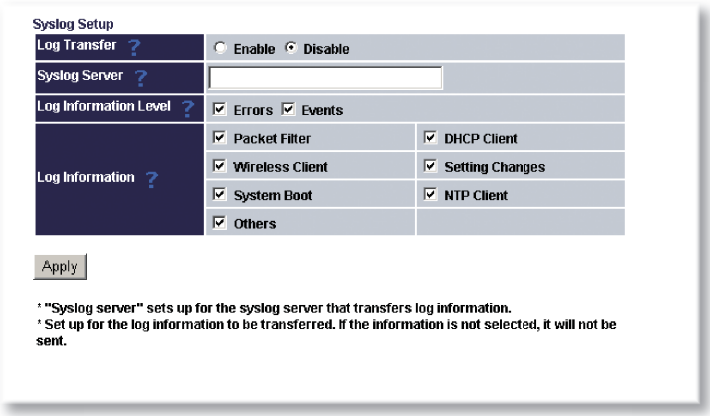


4.3.6 Log Information

Display Log Types - Select **Error** and/or **Notice** to specify the types of reports to be logged by the AirStation.

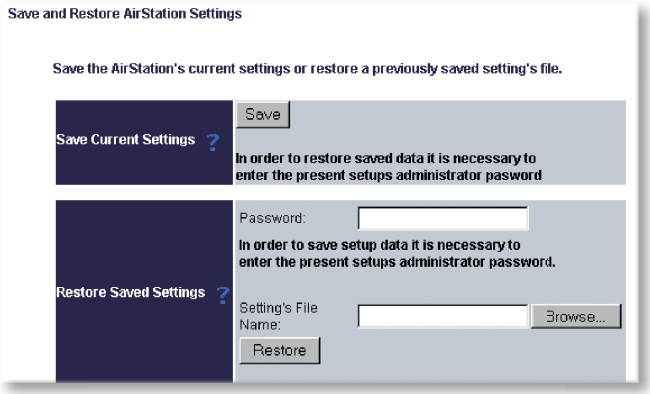
Display Log Infomation - Select the specific reports to be logged.

Log information - Displays recorded logs.



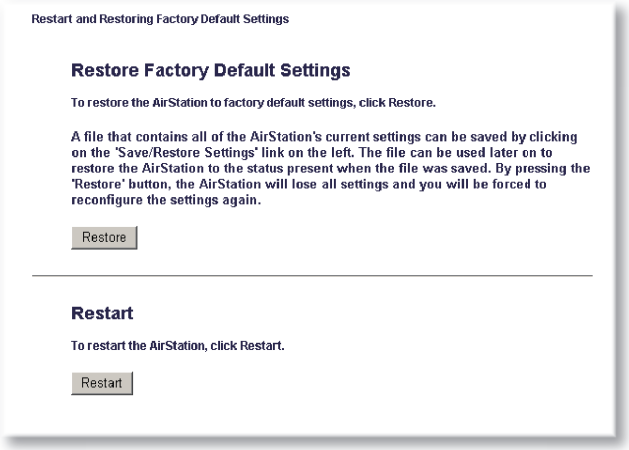
4.3.7 Syslog transmitting

Log Transfer - Select **Enable** or **Disable**
Syslog Server - Enter the IP address of the Syslog server.
Log Information Level - Select **Error** and/or **Notify** to specify the types of reports to be sent to the Syslog server.
Log Information - Select the specific reports to be sent to the Syslog server.


Save and Restore AirStation Settings
Save the AirStation's current settings or restore a previously saved setting's file.
Save Current Settings
Save
In order to restore saved data it is necessary to enter the present setups administrator pasword
Restore Saved Settings
Password:
In order to save setup data it is necessary to enter the present setups administrator password.
Setting's File Name:
Browse...
Restore

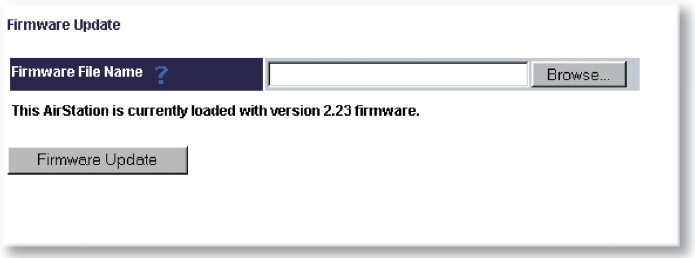
4.3.8 Save/Restore Settings

Save current setting to resume after losing or initializing setup information.


Restart and Restoring Factory Default Settings
Restore Factory Default Settings
To restore the AirStation to factory default settings, click Restore.
A file that contains all of the AirStation's current settings can be saved by clicking on the 'Save/Restore Settings' link on the left. The file can be used later on to restore the AirStation to the status present when the file was saved. By pressing the 'Restore' button, the AirStation will lose all settings and you will be forced to reconfigure the settings again.
Restore
Restart
To restart the AirStation, click Restart.
Restart

4.3.9 Initialization/Reboot

Initialization sets all parameters back to factory defaults. After initialization, the AirStation must be restarted.



4.3.10 Firmware Update

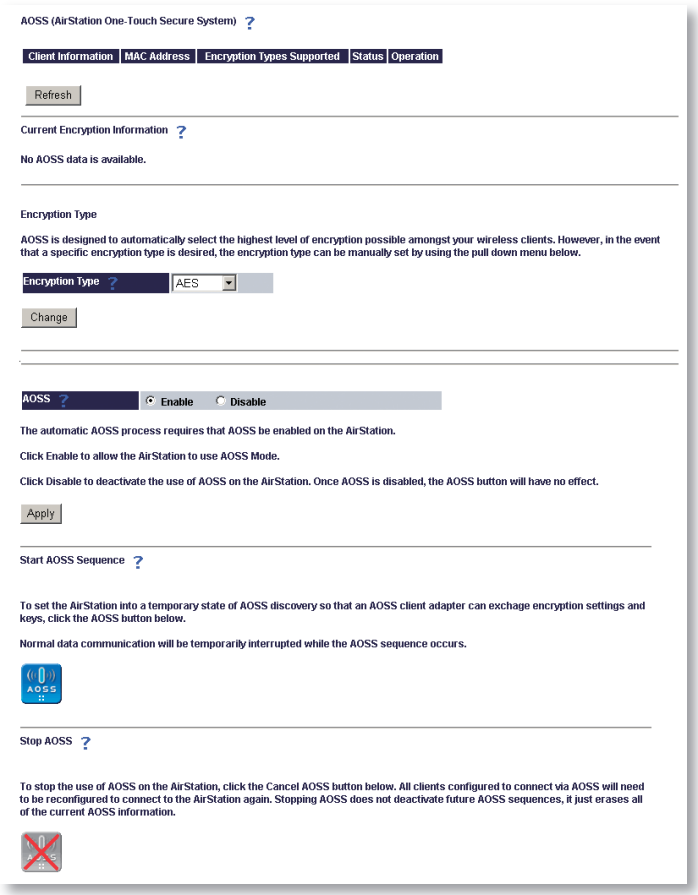
Firmware File Name - Enter the path and filename for new firmware or select **Browse** to search for the path.

Click **Firmware Update** to load firmware to the AirStation.

■ Note: Firmware update does not erase current user settings.

4.3.11 AOSS

AOSS (AirStation One-Touch Secure System) - Display the clients that are connected to the AirStation by A.O.S.S.


AOSS (AirStation One-Touch Secure System)
Client Information
MAC Address
Encryption Types Supported
Status
Operation
Refresh
Current Encryption Information
No AOSS data is available.
Encryption Type
AOSS is designed to automatically select the highest level of encryption possible amongst your wireless clients. However, in the event that a specific encryption type is desired, the encryption type can be manually set by using the pull down menu below.
Encryption Type
AES
Change
AOSS
Enable
Disable
The automatic AOSS process requires that AOSS be enabled on the AirStation.
Click Enable to allow the AirStation to use AOSS Mode.
Click Disable to deactivate the use of AOSS on the AirStation. Once AOSS is disabled, the AOSS button will have no effect.
Apply
Start AOSS Sequence
To set the AirStation into a temporary state of AOSS discovery so that an AOSS client adapter can exchage encryption settings and keys, click the AOSS button below.
Normal data communication will be temporarily interrupted while the AOSS sequence occurs.
AOSS
Stop AOSS
To stop the use of AOSS on the AirStation, click the Cancel AOSS button below. All clients configured to connect via AOSS will need to be reconfigured to connect to the AirStation again. Stopping AOSS does not deactivate future AOSS sequences, it just erases all of the current AOSS information.

- Name : Shows client's name.
- MAC address : Shows client's MAC address.
- Encryption type : Available encryption type of the client.
- Status : Shows current client's connection.
- Operation : Connect/disconnect the clients.

■ Note: Once disconnect button is clicked, the client's MAC address is listed in MAC filter table.

■ Note: The maximum number of MAC filer table is 64.

Current encryption Information - Display encryption level and security information.

- Security level : Current encryption level is displayed.
- SSID : Current SSID is displayed. Depending on encryption level.
- Encryption key/pre-shared key : Current encryption data. Depending on encryption level.

Encryption Type

Encryption level can be changed manually, when AOSS function is activated.

Confirm whether every clients can access before configuring this setting.

The following encryption levels can be selected.

(High security)AES - TKIP - WEP128 - WEP64(Low security)

Enable/disable AOSS button

AOSS

Enable/disable AOSS button.

• Enable : Enable A.O.S.S function.

• Disable : Disable A.O.S.S function.Exchange of AOSS. encryption keys can not be used until AOSS is enabled.

Start AOSS Sequence

Functions as an AOSS button on the AirStation unit.

The AirStation starts security key exchange, when the AOSS button is pushed.

The AOSS button is grayed out, when AOSS function is disabled.

Up to 24 clients are allow to connect to the AirStation by AOSS feature.

Stop AOSS

Clear AOSS configuration data.

USING AOSS

AOSS (AirStation One-Touch Secure System) is a simple, one-touch setup for connecting wireless clients to an access point while setting up the most secure possible connection.
Users no longer need to worry about choosing the proper security protocols, IP addresses, or SSID's. The intelligence of AOSS determines the most optimal connection and configures itself in seconds.

■ **NOTE:** AOSS automatically creates a secure connection between your AOSS Access Point and client. You must have a Buffalo AOSS enabled wireless client device to use the AOSS features of your AOSS Access Point/Router.

The INIT switch initiates AOSS mode now. If you want to restore the factory default settings, hold the INIT switch up to 5 seconds when turn the unit on.

◗ Configure your WLA2-G54C's network connection by referring to the above mentioned instructions.

◗ Once the WLA2-G54C has been configured, follow the directions to install your wireless client device and its drivers if necessary. Certain wireless client adapters require client software to configure them. If your device has a Client Manager, then install it as well.

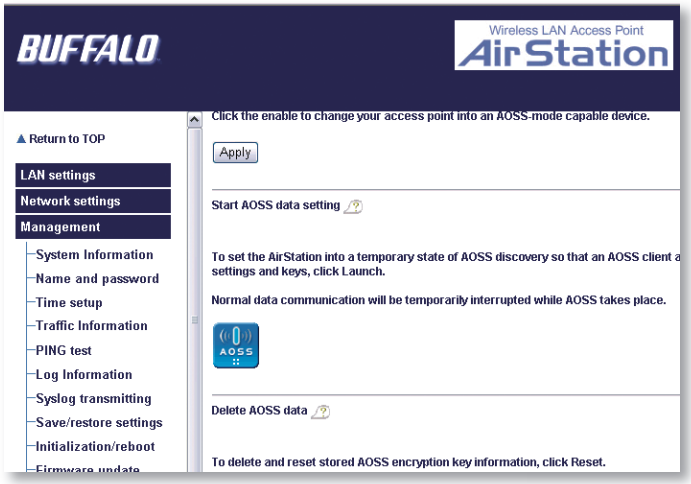
■ **NOTE:** If the wireless client adapter is installed on a PC, then the AOSS client manager will need to be installed as well. If your wireless client adapter is a standalone device that does not require a PC, then just power up the device.

Standalone Devices: Ethernet Converters and Access Point Bridges

Client Manager Devices: CardBus, USB, and PCI Adapters.

Standalone AOSS Device

Client Manager Device



◗ Now that the WLA2-G54C and wireless client adapter are installed, you can use AOSS to configure them.

◗ To begin the configuration, press the AOSS button in the WLA2-G54C's configuration. The AOSS menus can be found under the 'Advanced' Configuration, Management, AOSS. The status screen will briefly show that it is in AOSS mode. The WLA2-G54C's Wireless Light may turn on and off.

■ **NOTE:** AOSS mode will stay active for a period of two minutes. This is the time-slot required to initiate the wireless client adapter.

◗ Refer to your wireless client adapter's AOSS supplement to initiate the wireless client adapter's AOSS mode.

◗ Once the client adapter has begun communicating with the AOSS router, AOSS client will report a successful AOSS connection. This indicates that the AOSS process has begun and the two devices are configuring themselves. Please refer to your wireless client adapter's supplement for the remainder of the setup.

ADDITIONAL AOSS INFORMATION:

◗ Only one AOSS wireless client adapter can be configured to the AOSS access point at a time. Thus, the button will need to be repressed for each additional AOSS wireless client adapter that will be connected.

◗ It is not necessary to reconfigure AOSS client devices that have already been configured via AOSS, unless significant changes have been made to the wireless network.

◗ Do not attempt to configure two separate AOSS networks at the same time, as it may cause undesired configurations.

◗ If an undesired client has connected via AOSS, it can be disconnected from within the WLA2-G54C's advanced configuration AOSS menus.

ADDITIONAL INFORMATION

Please check the Buffalo Web site for the latest information and any corrections done for this manual.

For more information, please consult one of the following:

- The **on-line help system** of your AirStation wireless system - for information about software and driver functionality.
- The AirStation website at our local website indicated last page.
  - for frequently asked questions (FAQ's) and Software Updates.

Specifications

WLA2-G54C Physical Specifications

Dimensions (WxHxD) 56 x 120 x 92 mm

Weight: 0.56lbs (256g)

Temperature & Humidity

Operation 0 to 40 deg. C

Maximum humidity 80%

Transit/Storage 0 to 40 deg. C

Maximum humidity 80% (no condensation)

Power Characteristics

Transmit Mode 0.8A (Normal)

Power Supply 3.3V

Regulatory Information A

Wireless communication is often subject to local radio regulations. Although AirStation wireless networking products have been designed for operation in the license-free 2.4 GHz band, local radio regulations may impose limitations on the use of wireless communication equipment.

Networking Characteristics Compatibility

- IEEE 802.11 Standard for Wireless LANs (DSSS)
- Wi-Fi (Wireless Fidelity) certified by the Wi-Fi Alliance.

Host Operating System

Microsoft Windows® ME/98/NT4.0/2000/XP

Media Access Protocol

CSMA/CA (Collision Avoidance) with Acknowledgment (ACK)

Radio Characteristics (Typical Indoor Ranges)

R-F Frequency Band 2.4 GHz (2400-2483 MHz)

11 selectable sub-channels

Modulation Technique Direct Sequence Spread Spectrum

- CCK for High & Medium Transmit Rate
- DQPSK for Standard Transmit Rate
- DBPSK for Low Transmit Rate

Spreading 11-chip Barker Sequence

Bit Error Rate (BER) Better than 10 -5

Nominal Output Power 15 dBm (32mW)

Transmit Rate / Range

High Speed 54Mbps

Standard Speed 20 Mbps

Low Speed 1 Mbps

Open Office Environment

160 m (525 ft.)

270 m (885 ft.)

400 m (1300 ft.)

550 m (1750 ft.)Semi-Open Office Environment

50 m (165 ft.)

70 m (230 ft.)

90 m (300 ft.)

115 m (375 ft.)

Closed Office

25 m (80 ft.)

35 m (115 ft.)

40 m (130 ft.)

50 m (165 ft.)

Receiver Sensitivity -69dBm, -72dBm, -77dBm, -81dBm, -85dBm, -88dBm -87dBm -90 dBm -92 dBm (depends on data rate)

Delay Spread (at FER of <1%) 65 ns 225 ns 400 ns 500 ns (depends on data rate)

- The range of wireless devices can be affected by metal surfaces, solid high-density materials and obstacles in the signal path.
- In Open Office environments, clients can "see" each other, i.e. there are no physical obstructions between them.
- In Semi-open Office environments, work space is separated by room dividers; client cards are at desktop level.
- In Closed Office environments, workspace is separated by floor-to-ceiling brick walls.

NOTE:

The range values listed in Table "Radio Characteristics" are typical distances as measured at Buffalo Technology AirStation laboratories. These values are provided for your guidance but may vary according to the actual radio conditions at the location where the AirStation product is installed.

AirStation IEEE 802.11 Channel Sets

The range of the wireless signal is related to the Transmit Rate of the wireless communication. Communications at a lower Transmit range may travel longer distances.

Center Channel ID FCC

1 2412	7 2442
2 2417	8 2447
3 2422	9 2452
4 2427	10 2457
5 2432	11 2462 1
6 2437	1 default channel

B Troubleshooting

B.1 Common Troubleshooting Tips B

Common Problems:

• Out of range, client cannot connect to the AirStation.

• Configuration mismatch, client cannot connect to the AirStation.

• Absence or conflict with the Client Driver.

• Conflict of another device with the AirStation hardware.

B.1.1 LED Activity B

Monitoring LED activity helps identify problems.

- Power LED should be GREEN,

- Wireless LED should be GREEN if the line is active. If is it blinking GREEN, wireless communication is active.

- Ethernet LED should be GREEN (100Mbps) or AMBER (10Mbps) while the communication is active.

DIAG LED Activity

Unplug the power for three seconds. Plug the power back in to monitor the DIAG LEDs during start-up.

Table B.1.1

DIAG LED Activity Table

DIAG LED Display

Action - Description/Cause

Red flash, 3 times

Starting:

A problem in the wired LAN side

Red flash, 4 times

Starting:

A problem in the wireless LAN side

B. 1.2 LEDs Work But Client PC Cannot Connect to Network

If the LEDs indicate that the network is working properly (Power LED is on, Transmit/Receive LED blinks), check the TCP/IP settings of the network.

Changing Client TCP/IP Settings in Windows

Consult the LAN Administrator for TCP/IP settings.

To add or change the TCP/IP Settings:

1. On the Windows task bar click Start.

2. Select Settings, then Control Panel.

3. Double-click on the Network icon to view the Network Properties.

4. From the list of installed components, verify the TCP/IP -> Buffalo WLI-USB-L11G wireless LAN adapter protocol (or appropriate wireless LAN adapter) is installed.

• If this protocol is not yet installed, click the Add button and select the TCP/IP protocol from the list. Refer to Windows Help for more information.

• If this protocol is installed, select this protocol and click the Properties button. Verify the parameters match the settings provided by your LAN Administrator. Make changes if necessary, and click OK.

5. When prompted, restart your computer.

B. 1.3 Other Problems

Please refer to our local web site indicated last page.

Glossary

10BaseT or 100BaseTx: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 is 10 Mbps and 100 is 100 Mbps.

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network: The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Bandwidth: The transmission capacity of a computer or a communication channel, stated in Megabits per second (Mbps).

BSS (Basic Service Set): An 802.11 networking framework that includes an .

Bus Mastering: A system in which the specified Input/Output device (e.g. NIC Card) can perform tasks without the intervention of the CPU.

Client: A PC or workstation on a network.

Default Gateway: The IP Address of either the nearest bridge or server for the LAN.

Default Parameter: Parameter set by the manufacturer.

Destination Address: The address portion of a packet that identifies the intended recipient station.

DNS (Domain Name System): System used to map readable machine names into IP addresses

Driver: Software that interfaces a computer with a specific hardware device.

DSSS (Direct Sequence Spread Spectrum): Method of spreading a wireless signal into wide frequency bandwidth.

DTE (Data Terminal Equipment): Device that controls data flowing to and from a computer.

Dynamic IP Address: An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

ESS (Extended Service Set): A set of two or more BSSs that form a single sub-network. SSID is user identification used in the ESS LAN configuration.

Ethernet: The most widely used architecture for Local Area Networks (LANs). It is a shared-media network architecture. IEEE 802.3/802.3u standard details its functionality.

Ethernet cable: A wire similar to telephone cable that carries signals between Ethernet devices.

File and Print Sharing: A Microsoft application that allows computers on a network to share files and printers.

Firmware: Programming inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Full-Duplex: To transmit on the same channel in both directions simultaneously.

Half-duplex: To transmit on the same channel in both directions, one direction at a time.

Hub: A device which allows connection of computers and other devices to form a LAN.

IEEE (Institute of Electrical and Electronics Engineers): The professional organization which promotes development of electronics technology.

IP (Internet Protocol) Address: A unique 32-binary-digit number that identifies each sender or receiver of information sent in packets.

Infrastructure: A wireless network or other small network in which the wireless network devices are made a part of the network through the .

ISP (Internet Service Provider): A company that provides access to the Internet and other related services.

IV (Initialization Vector): The header section of a message packet.

LAN (Local Area Network): A group of computers and peripheral devices connected to share resources.

LED (Light Emitting Diode): The lights on a hardware device representing the activity through the ports.

MAC (Medium Access Control) Address: A unique number that distinguishes network cards.

Mbps (Mega Bits Per Second): A measurement of millions of bits per second.

MHz (MegaHertz): One million cycles per second.

NAT (Network Address Translation): An internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic.

NIC (Network Interface Card): An expansion card connected to a computer so the computer can be connected to a network.

Packet: A block of data that is transferred as a single unit, also called a frame or a block.

Packet Filtering: Discarding unwanted network traffic based on its originating address or its type.

Ping (Packet Internet Groper): An Internet utility used to determine whether a particular IP address is online.

Plug and Play: Hardware that, once installed ("plugged in"), can immediately be used ("played"), as opposed to hardware that requires manual configuration.

PoE (Power over Ethernet): A mechanism to send DC power to a device using a CAT5 Ethernet cable.

Protocol: A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service): A server that issues authentication key to clients.

Repeater Hub: A device that collects, strengthens and transmits information to all connected devices, allowing the network to be extended to accommodate additional workstations.

RC4: The encryption algorithm that is used in WEP.

RJ-45 connector: An 8-pin connector used between a twisted pair cable and a data transmission device.

Bridge: Device that can connect individual LANs and remote sites to a server.

Roaming: The ability to use a wireless device while moving from one to another without losing the connection.

SMTP (Simple Mail Transfer Protocol): The protocol used to define and deliver electronic mail (e-mail) from one location to another.

SNMP (Simple Network Management Protocol: An application layer protocol that outlines the formal structure for communication among network devices.

Static IP Address: A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

Subnet Mask: An eight-byte address divided into 4 parts separated by periods.

TCP/IP (Transmission Control Protocol/Internet Protocol: Protocol used by computers when communicating across the Internet or Intranet.

TKIP (Temporal Key Integrity Protocol): An encryption method replacing WEP. TKIP uses random IV and frequent key exchanges.

UDP (User Datagram Protocol): A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

Static IP Address: A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

Subnet Mask: An eight-byte address divided into 4 parts separated by periods.

WAN (Wide Area Network): A networking system covering a wide geographical area.

WEP (Wired Equivalent Privacy): An encryption method based on 64 or 128bit algorithm.

Web Browser: A software program that allows viewing of web pages.

Wi-Fi (Wireless Fidelity): An organization that tests and assures interoperability among WLAN devices.

Wire Speed: The maximum speed at which a given packet can be transferred using Ethernet and Fast Ethernet standard specifications.

WLAN (Wireless LAN): A LAN topology using wireless devices.

WPA (Wi-Fi Protected Access): An encryption method replacing WEP.

VPN (Virtual Private Network): A security method to connect remote LAN users to a corporate LAN system.

FCC/CE / R&TTE

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of the DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of compliance with the R&TTE Directive 1999/5/EC:

- EN 60950: 2000
Safety of Information Technology Equipment

- EN 300 328-2 V1.2.1 (2001-12)
Technical requirements for spread-spectrum radio equipment

- EN 301 489-17 V1.1.1 (2000-09)
EMC requirements for spread-spectrum radio equipment.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

Intended use

This device is a 2.4 GHz wireless LAN transceiver, intended for indoor home and office use in all EU and EFTA member states.

EU Countries intended for use

This device is intended for indoor Home and office use in the following countries:
Austria, Belgium, Germany, Denmark, Spain, Greece, France, Finland, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Sweden, United Kingdom, Cyprus, Czech Republic, Estonia, Hungry, Latvia, Lithuania, Malta, Poland, Slovak Republic and Slovenia.

The device is also authorised for use in all EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not intended for use

None.

Potential restrictive use

France: Only channels 10,11,12, and13

Potential restrictive use

This device is a 2.4 GHz wireless LAN transceiver, intended for indoor home and office use in all EU and EFTA member states, except in France, Belgium
and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain an authorization to use the device for setting up outdoor radio links.

In Belgium there is a restriction in outdoor use. The frequency range in which outdoor operation in Belgium is permitted is 2460 – 2483.5 MHz.

This device may not be used for setting up outdoor radio links in France. For more information see http://www.anfr.fr/ and/or http://www.art-telecom.fr

BUFFALO WARRANTY STATEMENT

Buffalo products come with a 2-year limited warranty from the date of purchase.
Buffalo Technology warrants in good operating condition for the warranty period. This warranty does not include non-Buffalo Technology installed components. If the Buffalo product malfunctions during the warranty period, Buffalo Technology will, at its discretion, repair or replace the product at no charge, provided the product has not been subjected to misuse, abuse or non-Buffalo Technology authorized alterations, modifications or repairs. When returning a product, include your original proof of purchase. Return requests cannot be processed without proof of purchase. Shipment of returned product to Buffalo Technology is the responsibility of the purchaser. All expressed and implied warranties for the Buffalo product line including, but not limited to, the warranties of merchantability and fitness for a particular purpose, are limited in duration to the above period.

Under no circumstances shall Buffalo Technology be liable in any way to the user for damages, including any lost profits, lost savings or other incidental or consequential damages arising out of the use of, or inability to use, the Buffalo products.

Buffalo Technology reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Important Notice
Please have your proof of purchase receipt to get warranty support. All defective products shall be returned with a copy of proof of purchase.
In no event shall Buffalo Technology's liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. Buffalo Technology does not offer refunds for any product.

MEMO

MEMO

MEMO